Como importar certificado nos switches Sx350 e Sx50X Series

Objetivo

Este objetivo deste documento é fornecer as etapas para importar com êxito um certificado nos switches das séries Sx350 e Sx550X usando a Interface Gráfica do Usuário (GUI - Graphical User Interface) e a Interface de Linha de Comando (CLI - Command Line Interface).

Table Of Contents

Introduction

Um dos problemas encontrados ao importar um certificado em switches Sx350 e Sx550X é que o usuário enfrenta ***o cabeçalho da chave ausente*** e/ou ***falha ao carregar*** erros ***de chave pública***. Este documento explicará como ultrapassar esses erros para importar com êxito um certificado. Um certificado é um documento eletrônico que identifica um indivíduo, um servidor, uma empresa ou outra entidade e associa essa entidade a uma chave pública. Os certificados são usados em uma rede para fornecer acesso seguro. Os certificados podem ser autoassinados ou assinados digitalmente por uma autoridade de certificação externa (AC). Um certificado autoassinado, como o nome indica, é assinado por seu próprio criador. As CAs gerenciam solicitações de certificado e emitem certificados para entidades participantes, como hosts, dispositivos de rede ou usuários. Um certificado digital assinado por CA é considerado padrão do setor e mais seguro.

Dispositivos aplicáveis e versão de software

- SG350 versão 2.5.0.83
- SG350X versão 2.5.0.83
- SG350XG versão 2.5.0.83
- SF350 versão 2.5.0.83
- SG550X versão 2.5.0.83
- SF550X versão 2.5.0.83
- SG550XG versão 2.5.0.83
- SX550X versão 2.5.0.83

Prerequisites

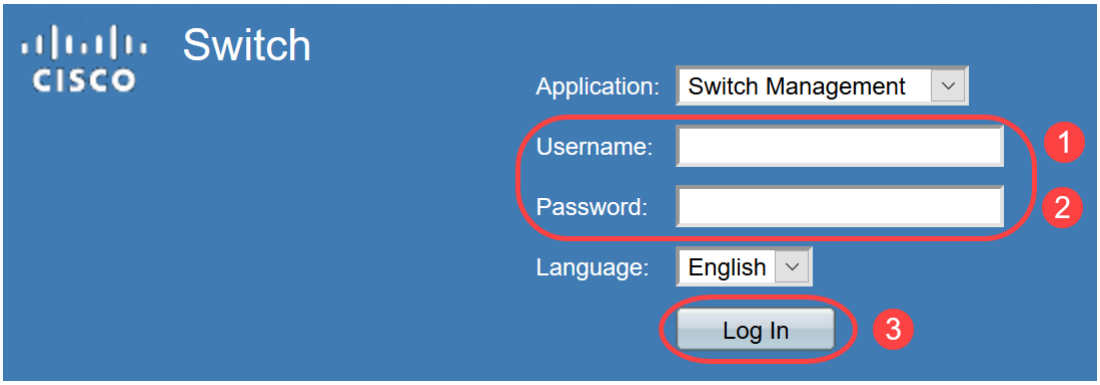
Você deve ter um certificado de Autoridade de Certificação (CA) ou autoassinado. As etapas para obter um certificado autoassinado estão incluídas neste artigo. Para saber mais sobre certificados

CA, clique aqui.

Importar usando GUI

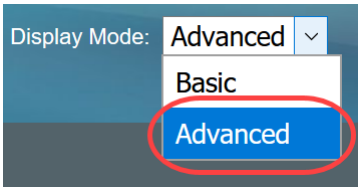
Passo 1

Faça login na GUI do switch digitando seu *nome de usuário* e *senha*. Clique em **Login**.



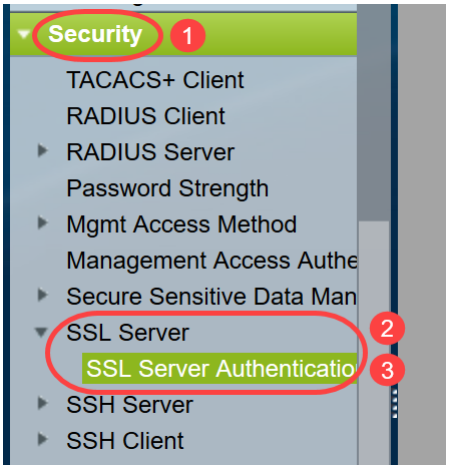
Passo 2

No *Modo de exibição* na parte superior direita da GUI, escolha **Avançado** usando a opção suspensa.



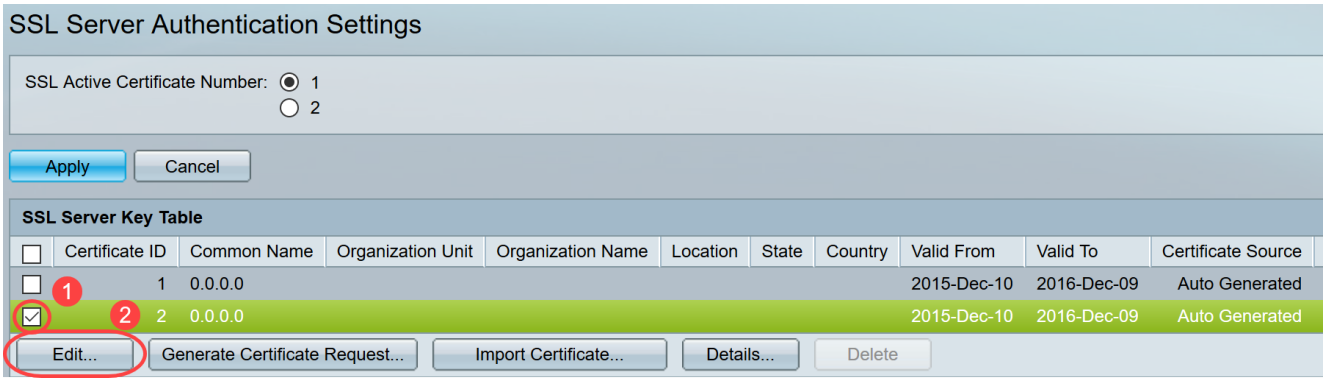
Etapa 3

Navegue até **Security > SSL Server > SSL Server Authentication**.



Passo 4

Selecione um dos certificados que é *gerado automaticamente*. Selecione a *ID de certificado* 1 ou 2 e clique no botão **Editar**.



Etapa 5

Para gerar um certificado autoassinado, na nova janela pop-up, habilite *Recriar chave RSA* e insira os seguintes parâmetros:

Comprimento da chave

Nome comum

Unidade organizacional

Nome da organização

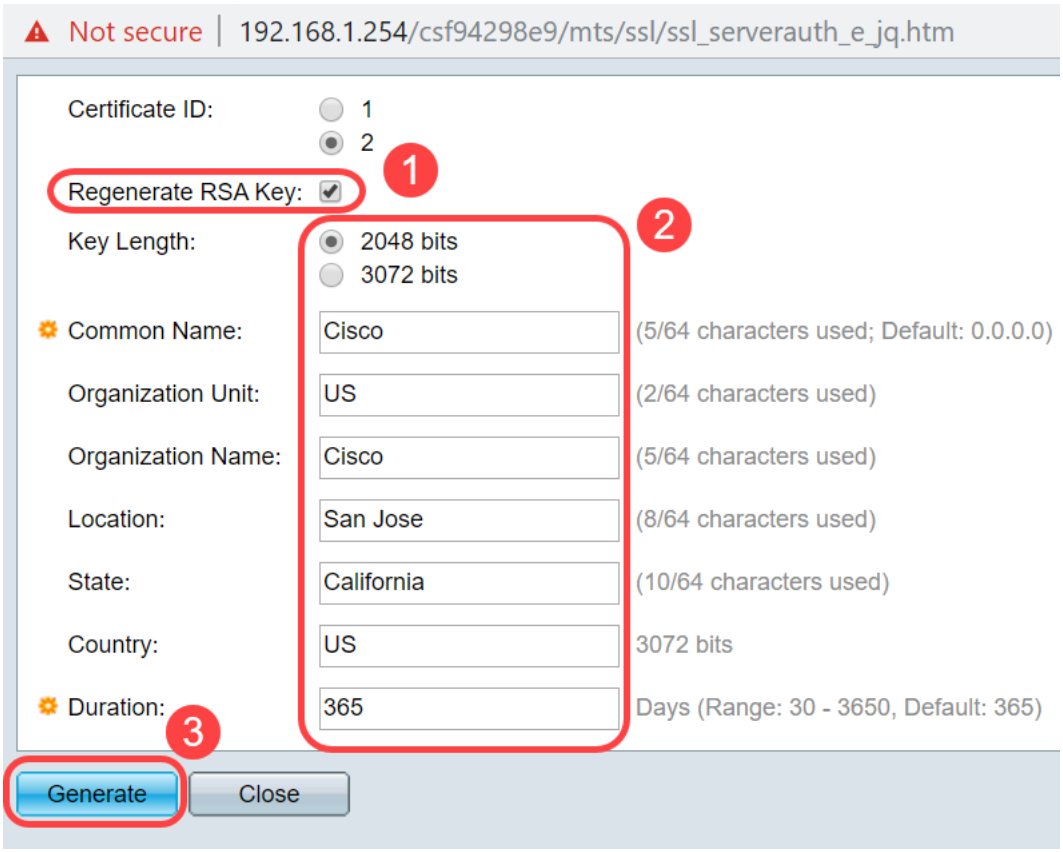
Local

Estado

País

Duration

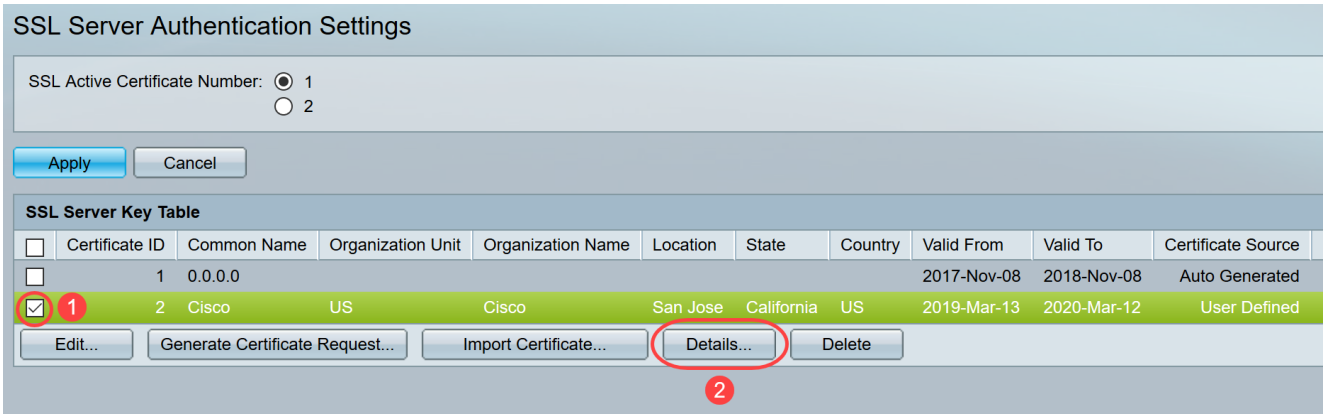
Clique em **Gerar**.



Você também pode criar um certificado de uma CA de terceiros.

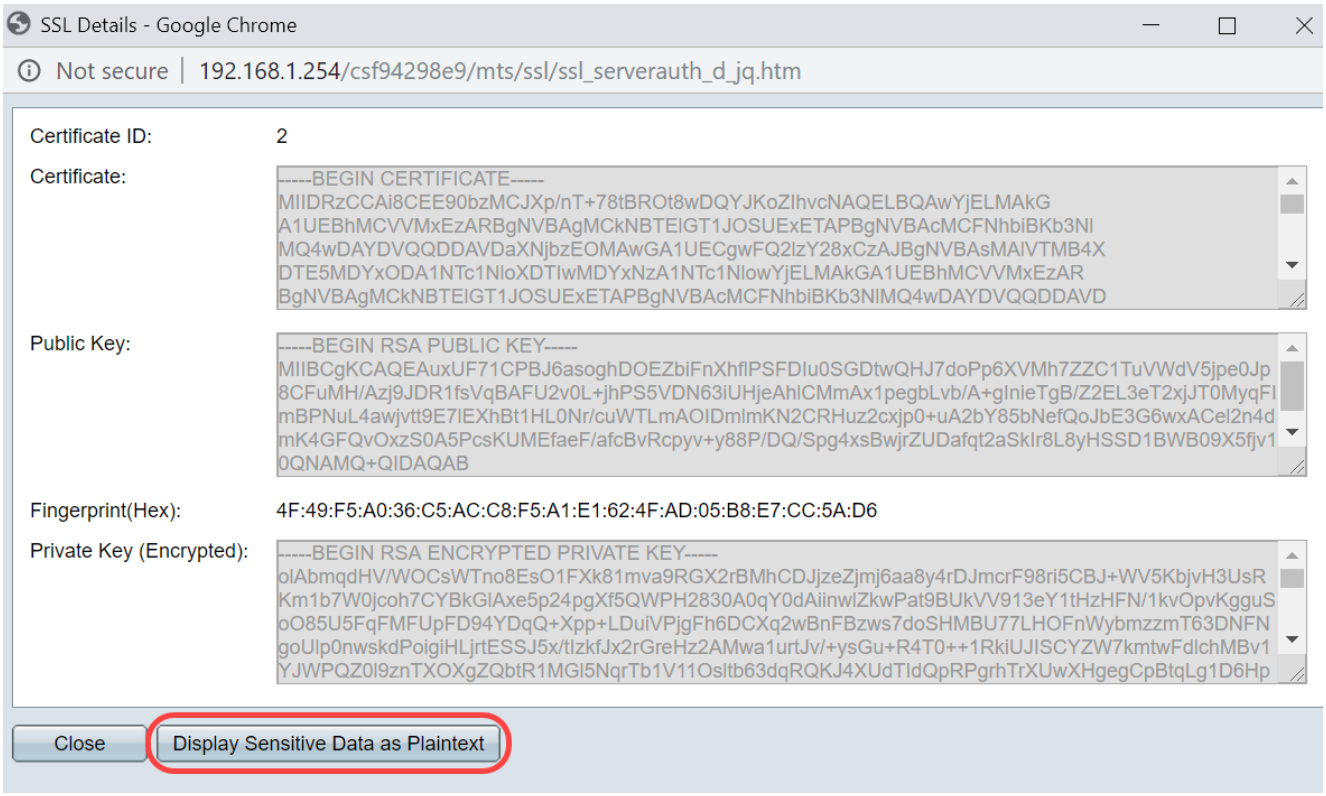
Etapa 6

Agora você poderá ver o certificado *definido pelo usuário* na *Tabela de chaves do servidor SSL*. Selecione o certificado recém-criado e clique em **Detalhes**.



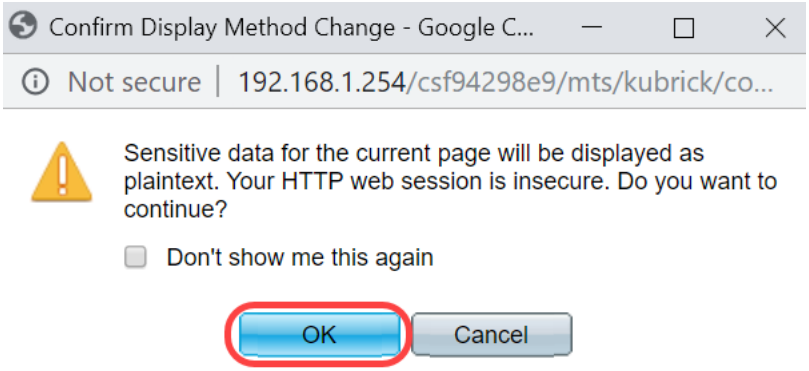
Etapa 7

Na janela pop-up, você poderá ver os detalhes *Certificado*, *Chave pública e Chave privada (criptografada)*. Você pode copiá-los em um arquivo do bloco de notas separado. Clique em **Exibir dados confidenciais como texto sem formatação**.



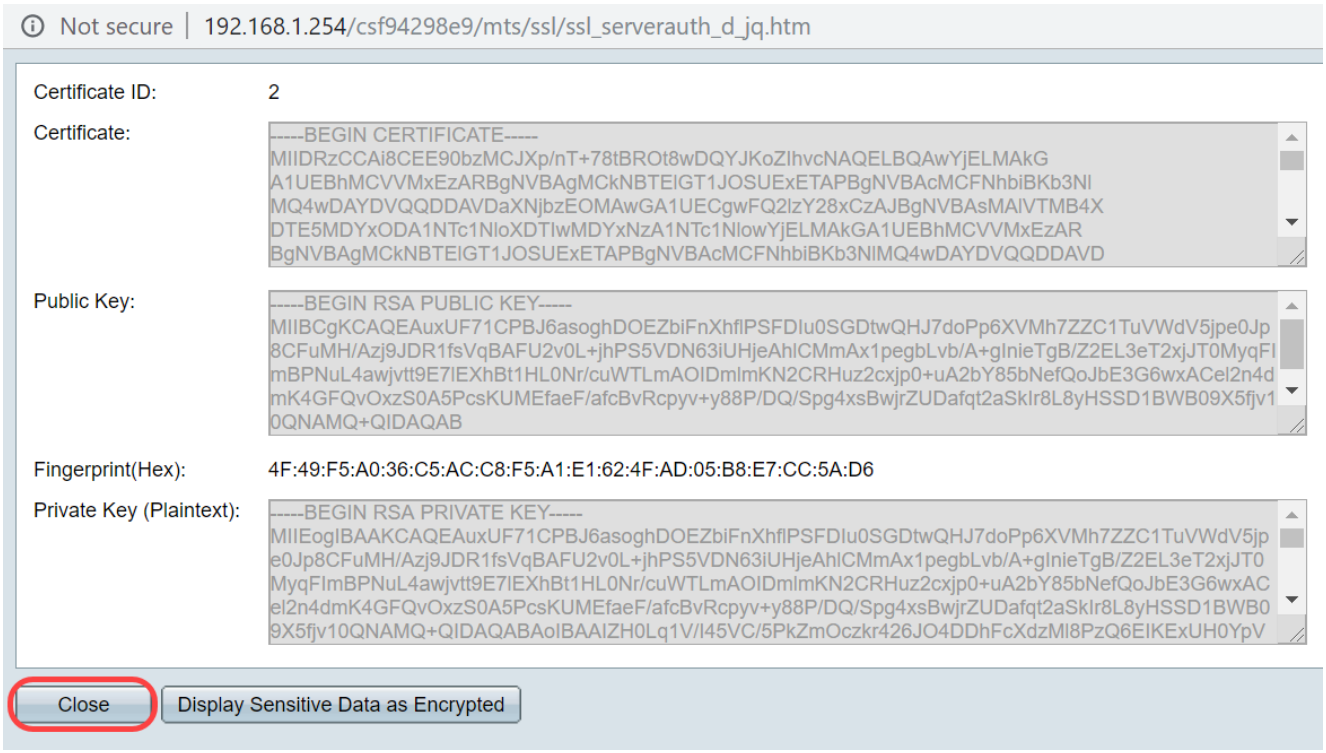
Passo 8

Uma janela pop-up será aberta para confirmar a exibição da chave privada como texto não criptografado e clique em **OK**.



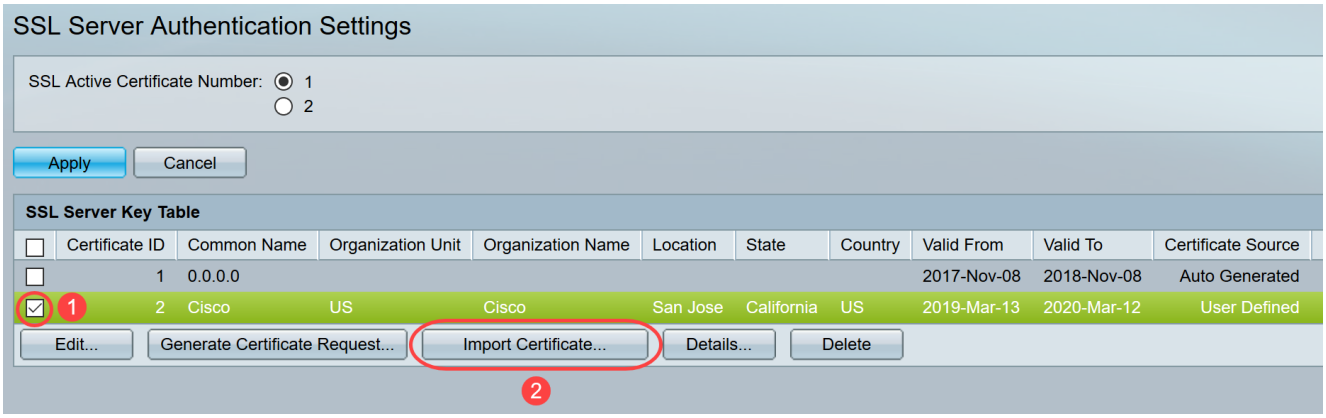
Passo 9

Agora você poderá ver a *chave privada* no formato de texto simples. Copie essa saída de texto simples em um arquivo do bloco de notas. Clique em Close.



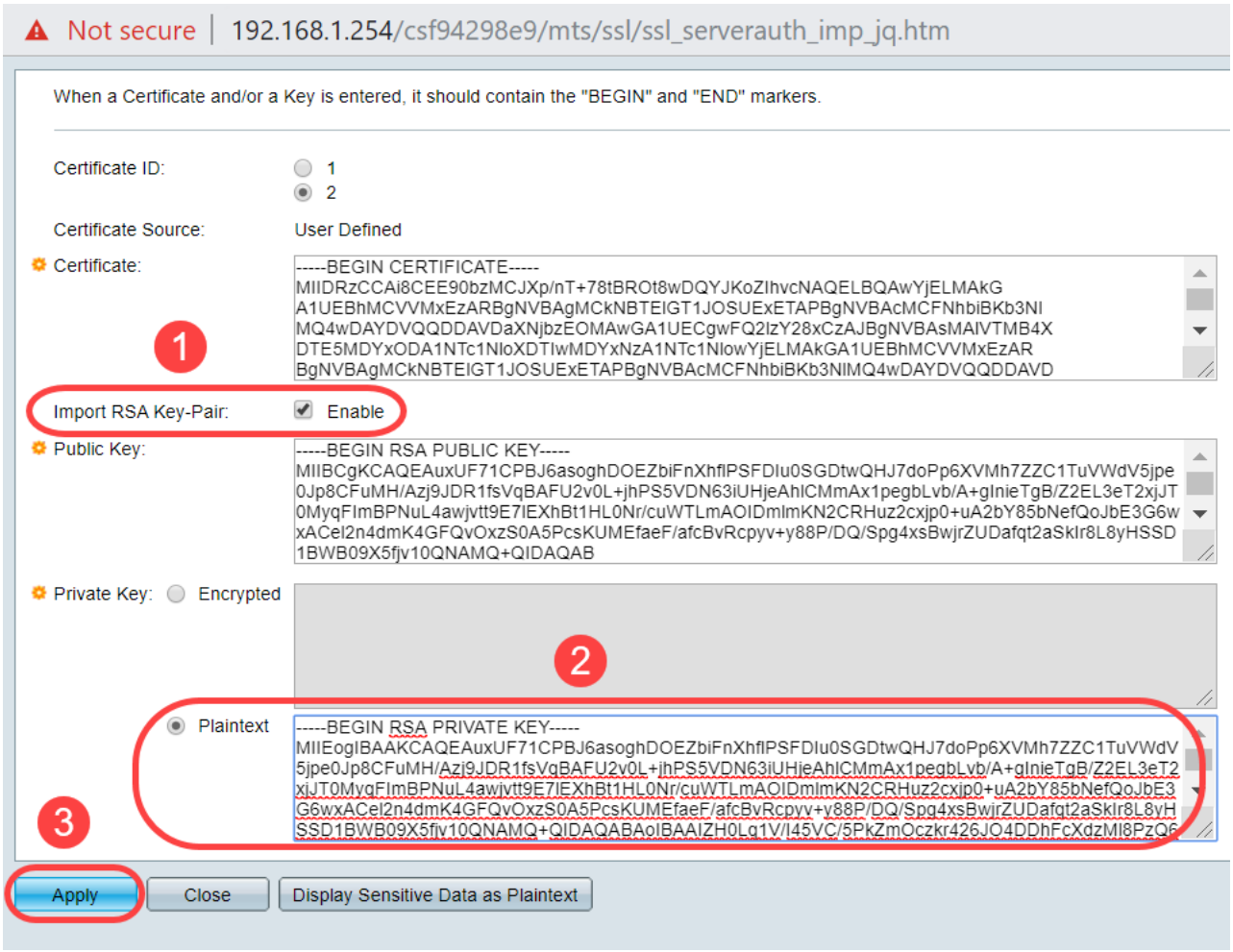
Passo 10

Selecione o certificado *definido pelo usuário* recém-criado e clique em **Importar certificado**.



Passo 11

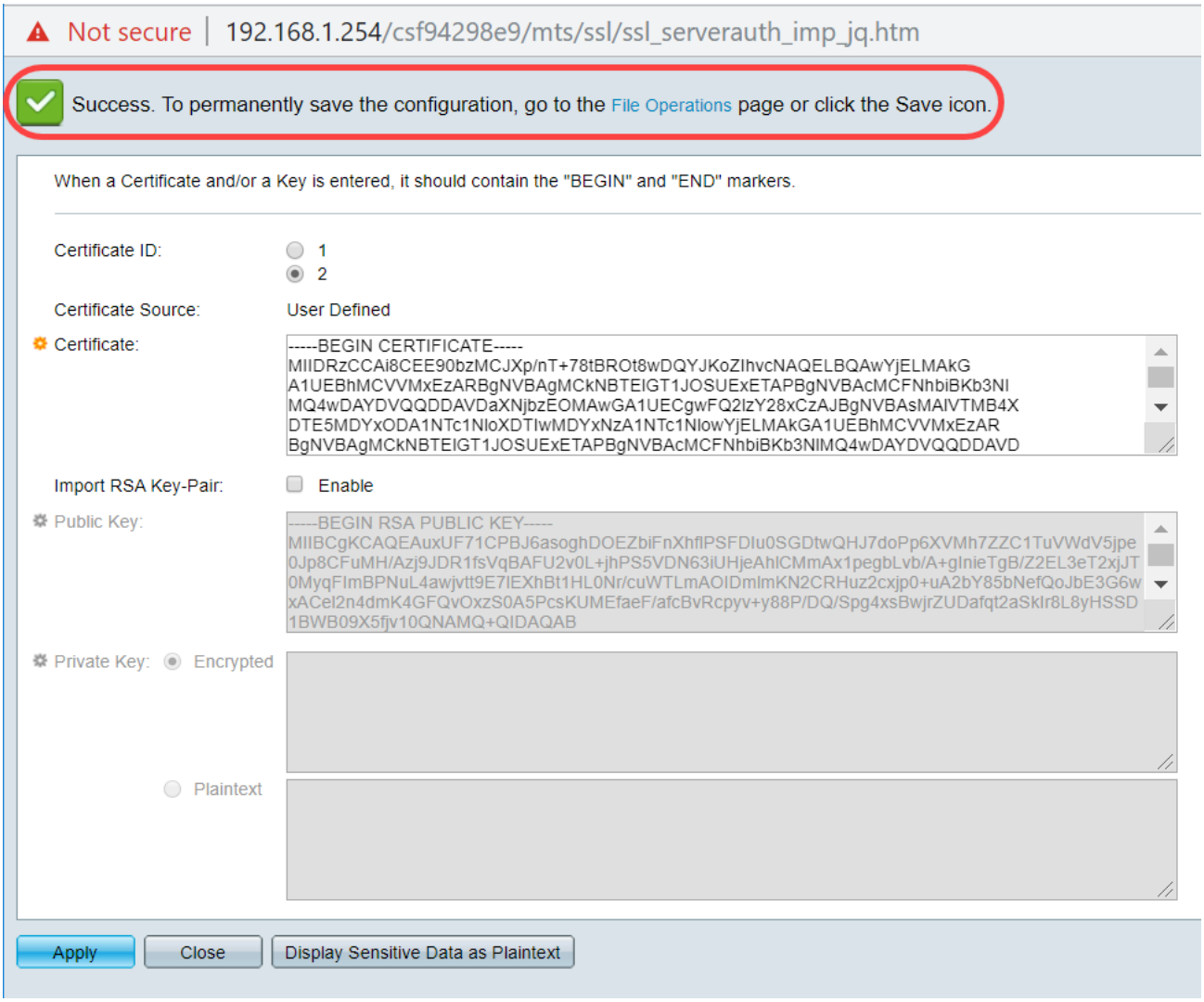
Na nova janela pop-up, ative a opção *Importar par de chaves RSA* e cole a chave privada (copiada na etapa 9) no formato de texto simples. Clique em Apply.



Neste exemplo, a palavra-chave, *RSA*, está incluída no *BEGIN* e *END* da *chave pública*.

Etapa 12

Você verá a notificação de sucesso na tela. Você pode fechar esta janela e salvar a configuração no switch.



Possíveis erros

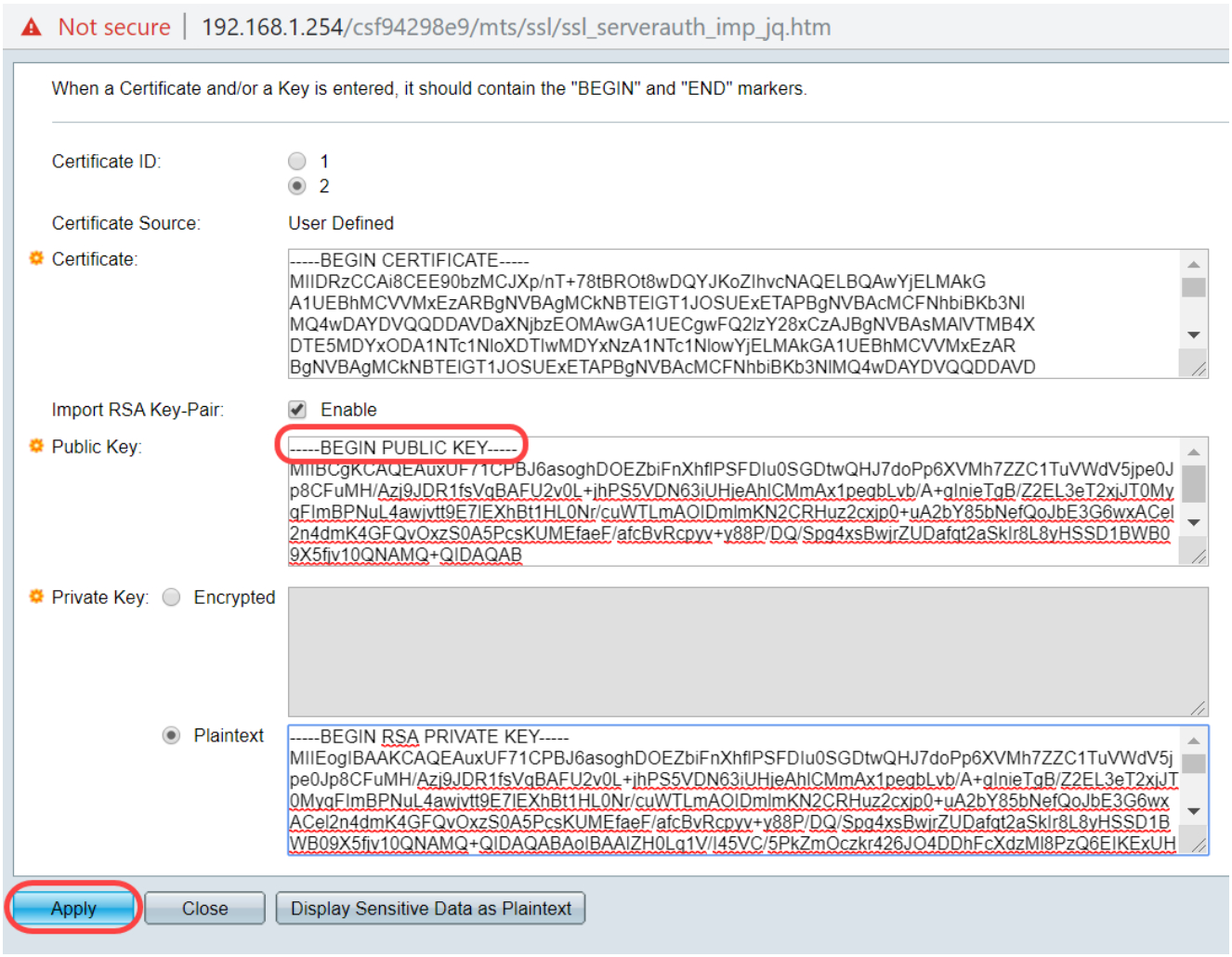
Os erros discutidos pertencem à chave pública. Normalmente, há dois tipos de formatos de chave pública que são usados:

1. Arquivo de chave pública RSA (PKCS#1): Isso é específico para chaves RSA.
Começa e termina com as marcas:
—INICIAR A CHAVE PÚBLICA RSA—
DADOS CODIFICADOS BASE64
—ENCERRA A CHAVE PÚBLICA RSA—

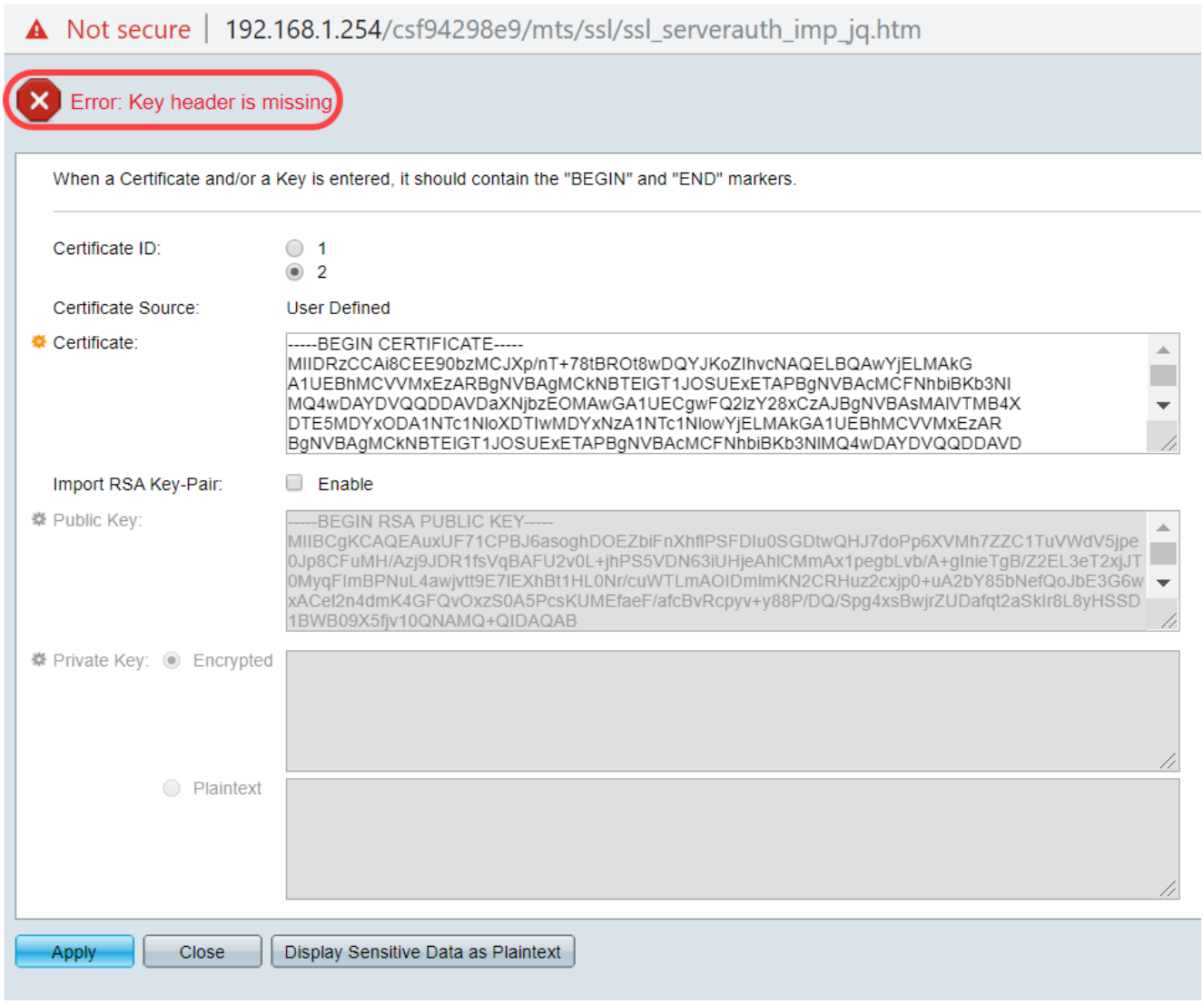
2. Arquivo de chave pública (PKCS#8): Trata-se de um formato de chave mais genérico que identifica o tipo de chave pública e contém os dados relevantes.
Começa e termina com as marcas:
—INICIAR CHAVE PÚBLICA—
DADOS CODIFICADOS BASE64
—CHAVE PÚBLICA FINAL—

Erro de cabeçalho de chave ausente

Cenário 1: Você gerou o certificado de uma CA de terceiros. Você copiou e colou a chave pública e clicou em **Aplicar**.



Você recebeu a mensagem, *Erro: Cabeçalho da chave ausente*. Feche a janela. Algumas modificações podem ser feitas para que esse problema desapareça.

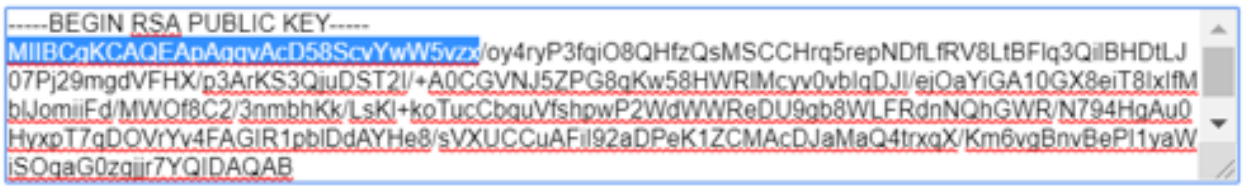


Para corrigir este erro:

Adicione a palavra-chave, *RSA*, ao início da chave pública: *INICIAR CHAVE PÚBLICA* ***RSA***

Adicione a palavra-chave, *RSA*, ao fim da chave pública: *CHAVE PÚBLICA FINAL* ***RSA***

Remova os primeiros 32 caracteres do código de chave. A parte destacada abaixo é um exemplo dos primeiros 32 caracteres.

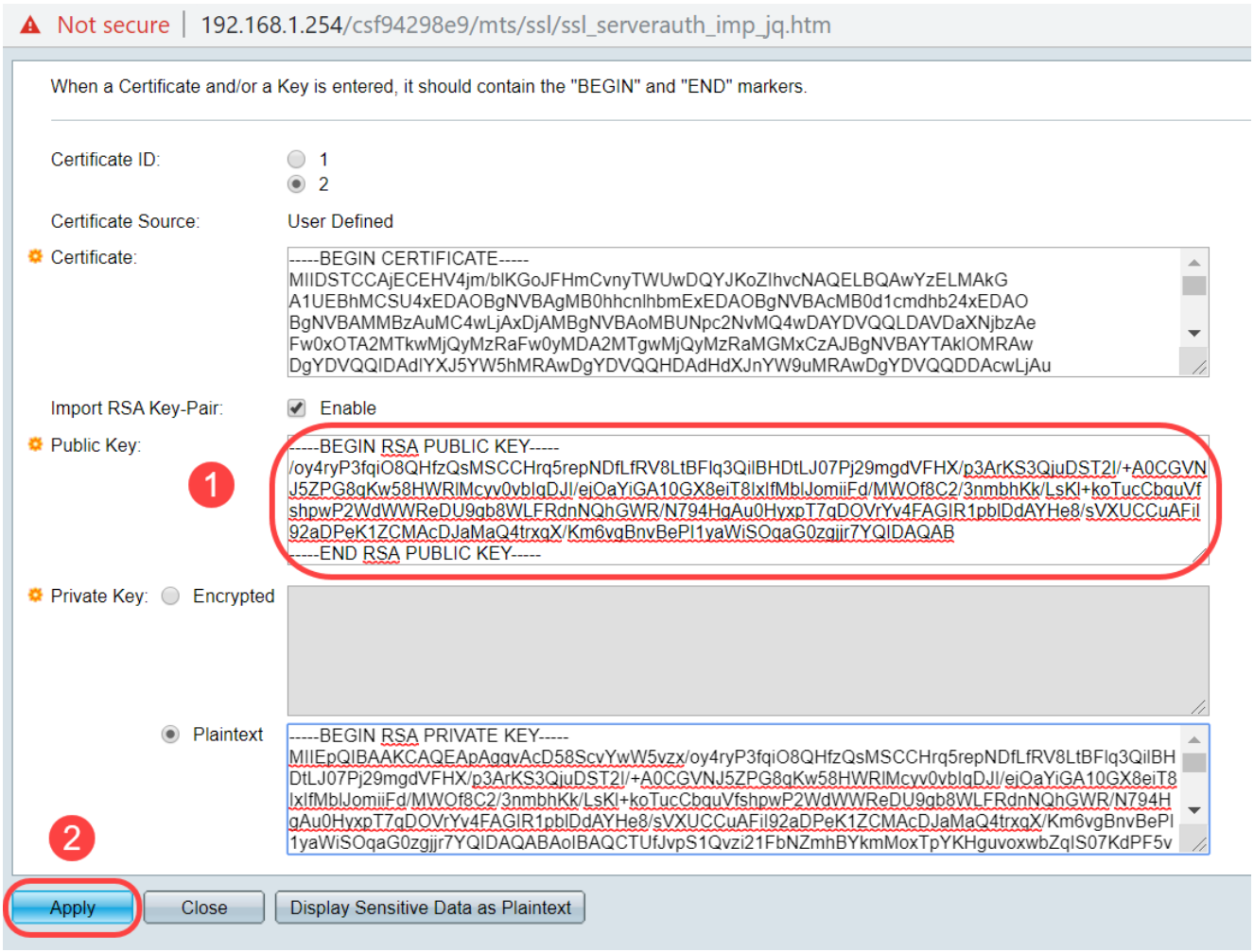


Ao aplicar as configurações, você não obterá o erro *Cabeçalho da chave ausente* na maioria dos casos.

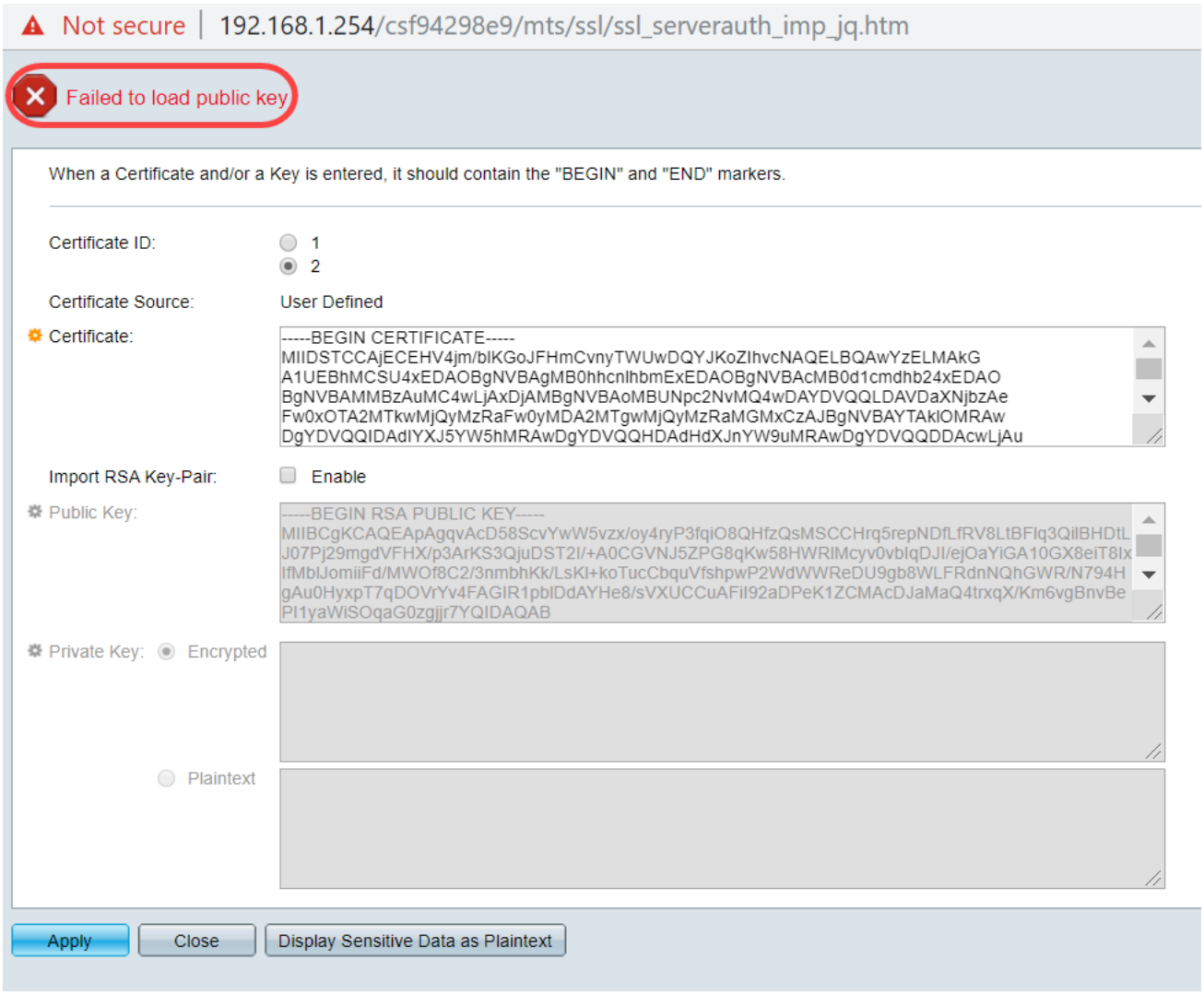
Falha ao carregar erro de chave pública

Cenário 2: Você gerou um certificado em um switch e o importou em outro switch. Você copiou e

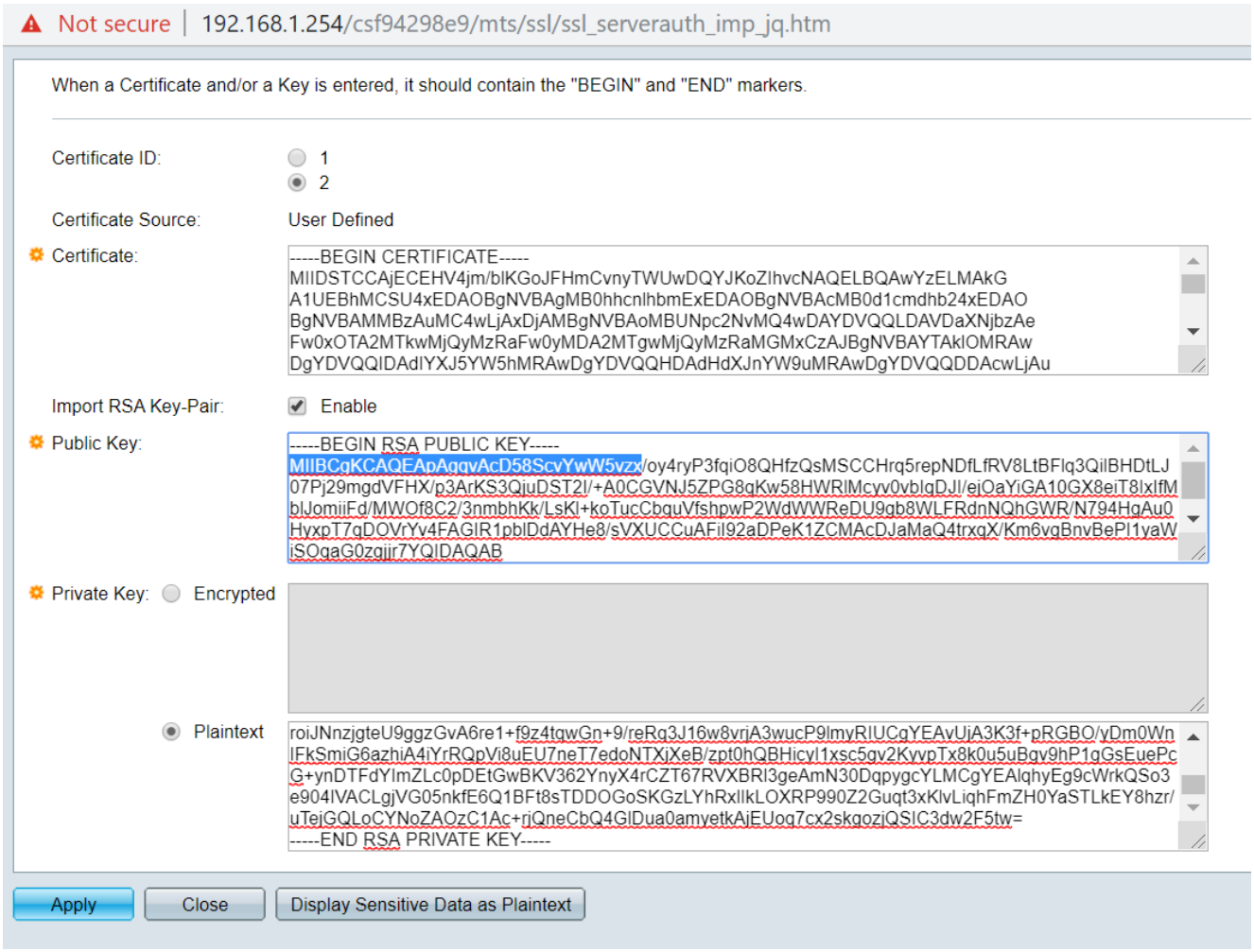
colou a chave pública após remover os primeiros 32 caracteres e clicar em **Aplicar**.



Você recebeu o erro *Falha ao carregar chave pública* na tela.



Para corrigir esse erro, NÃO exclua os primeiros 32 caracteres da chave pública nesse caso.



Importar usando CLI

Passo 1

Para importar certificado usando CLI, digite o seguinte comando.

```
switch(config)#crypto certificate [número do certificado] import
```

O certificado 2 é importado neste exemplo.

```
switch(config)#crypto certificate 2 import
```

Passo 2

Colar a entrada; **adicione um ponto (.)** em uma linha separada após a entrada.

```
—INICIAR A CHAVE PRIVADA RSA—
MIIEvgIBADANBgkqhkiG9w0BAQEFAASCBKgwggSkAgEAAoIBAQC/rZQ6f0rj8neA
...truncada 24 linhas....
h27Zh+aWX7dxakaoF5QokBTqWDHcMAvNluwGiZ/O3BQYgSiI+SYrZXAbUiSvfIR4
NC1WqkWzML6jW+52lD/GokmU
—ENCERRA A CHAVE PRIVADA RSA—
—INICIAR A CHAVE PÚBLICA RSA—
MIIBCgKCAQEAv62UOn9K4/J3gCAk7i9nYL5zYm4kQVQhCcAo7uGblEprxdWkfT0l
...truncada 3 linhas....
64jc5fzIfNnE2QpgBX/9M40E41BX5Z0B/QIDAQAB
```

```
—ENCERRA A CHAVE PÚBLICA RSA—
—INICIAR CERTIFICADO—
MIIFvTCCBKWgAwIBAgIRAOOBWg4bkStdWPvCNYjHpbYwDQYJKoZIhvcNAQELBQAw
—truncada 28 linhas...
8S+39m9wPAOZipI0JA1/0IeG7ChLWOXKncMeZWVTIUZaEwVFf0cUzqXwOJcsTrMV
JDPtnbKXG56w0Trecu6UQ9HsUBoDQnlsN5ZBHt1VyjAP
—CERTIFICADO FINAL—
.
Certificado importado com êxito
Emitido por: C=xx, ST=Gxxxx, L=xx, O=xx CA Limited, CN=xx RSA Organization Validation Secure
Server CA
Válido de: Jun 14 00:00:00 2017 GMT
Válido para: 11 de setembro 23:59:59 2020 GMT
Assunto: C=DE/postalCode=xxx, ST=xx, L=xx/street=xxx 2, O=xxx, OU=IT, CN=*.kowi.eu
Impressão digital SHA: xxxxxx
```

Conclusão

Agora você aprendeu as etapas para importar com êxito um certificado nos switches das séries Sx350 e Sx550X usando a GUI e a CLI.